March 25, 2005

ENGROSSED
SENATE BILL No. 49

DIGEST OF SB 49 (Updated March 23, 2005 4:08 pm - DI 69)

Citations Affected: IC 4-6; IC 23-15; IC 24-4.8; IC 35-32; IC 35-41.

Synopsis: Various computer issues. Requires state agencies and business entities to disclose any breach of the security of computerized data systems maintained by the agencies and entities to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Prohibits certain uses of spyware. Authorizes a provider of computer software, a web site owner, or a trademark or copyright holder harmed by a prohibited use of spyware to bring a civil action against the person who committed the prohibited act. Allows a person who brings a cause of action for unlawful spyware installation to receive injunctive relief and the greater of actual damages or $100,000 per violation. Provides that a person may be convicted of an offense if the person's conduct constitutes an offense under Indiana law and either: (1) involves the use of the Internet or another computer network, and access to the Internet or other computer network occurs in Indiana; or (2) involves

(Continued next page)

Effective: July 1, 2005.

Ford, Drozda, Broden, Hershman

(HOUSE SPONSOR — KOCH)

January 4, 2005, read first time and referred to Committee on Judiciary.
January 13, 2005, reported favorably — Do Pass.
January 18, 2005, read second time, ordered engrossed.
January 19, 2005, engrossed.
January 20, 2005, read third time, passed. Yeas 42, nays 0.

HOUSE ACTION

March 7, 2005, read first time and referred to Committee on Courts and Criminal Code.
March 24, 2005, amended, reported — Do Pass.

the use of electronic communication, including the Internet or another computer network, outside Indiana and the victim of the conduct resides in Indiana at the time of the conduct. Provides that a trial for such conduct may be held in a county: (1) from which or to which access to the Internet or other computer network was made; (2) in which any computer, computer data, computer software, or computer network that was used to access the Internet or other computer network is located; or (3) in which the victim resides at the time of the conduct if the conduct involves the use of electronic communication and occurs outside Indiana, and the victim resides in Indiana at the time of the conduct.

March 25, 2005

First Regular Session 114th General Assembly (2005)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type.~~

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.

Conflict reconciliation: Text in a statute in *this style type* or ~~*this style type*~~ reconciles conflicts between statutes enacted by the 2004 Regular Session of the General Assembly.

ENGROSSED
SENATE BILL No. 49

A BILL FOR AN ACT to amend the Indiana Code concerning computer issues.

Be it enacted by the General Assembly of the State of Indiana:

SECTION 1. IC 4-6-6.5 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]:

Chapter 6.5. State Agency Computer System Security Breaches

Sec. 1. (a) As used in this chapter, "breach of the security of the system" means the unauthorized acquisition of computerized data from a computerized data system that compromises the security, confidentiality, or integrity of personal information maintained by a state agency.

(b) The term does not include a good faith acquisition of personal information by an employee or agent of a state agency for agency purposes if the personal information is not used for or subject to further unauthorized disclosure.

Sec. 2. (a) As used in this chapter, "personal information" means:

(1) an individual's unencrypted:

(A) first name or first initial; and

(B) last name; and

(2) at least one (1) of the following:

(A) The individual's unencrypted Social Security number.

(B) The individual's unencrypted driver's license number or identification card number issued under IC 9-24.

(C) The individual's unencrypted:

(i) account number; or

(ii) credit or debit card number;

combined with a required security code, access code, or password that would allow access to the individual's financial account.

(b) The term does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Sec. 3. (a) A state agency that owns or licenses a computerized data system that includes personal information shall disclose any breach of the security of the system after the discovery of the breach to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(b) Subject to section 5 of this chapter, a disclosure made under subsection (a) must be made as soon as possible after the breach is discovered consistent with any measures taken by the state agency that are necessary to:

(1) determine the scope of the breach; and

(2) restore the reasonable integrity of the data system.

Sec. 4. Subject to section 5 of this chapter, a state agency that maintains a computerized data system that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following the discovery of the breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Sec. 5. The notification required under sections 3 and 4 of this chapter:

(1) may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; and

(2) shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

Sec. 6. (a) For purposes of sections 3 and 4 of this chapter, notice may be provided by any of the following methods:

(1) Written notice.

(2) Electronic notice if the notice provided is consistent with provisions concerning electronic records and signatures set forth in 15 U.S.C. 7001 et seq.

(3) Another form of notice if the state agency demonstrates that providing notice under subdivisions (1) and (2) would cost more than two hundred fifty thousand dollars ($250,000) or require more than five hundred thousand (500,000) persons to be notified or if the agency does not have sufficient contact information. Notice provided under this subdivision must include all the following:

(A) Electronic mail notice, if the agency has an electronic mail address for a person that must be notified.

(B) If the agency maintains an Internet web site, conspicuous posting of the notice on the agency's web site.

(C) Notification to major statewide news media.

(b) Notwithstanding subdivision (a), a state agency that maintains its own notification procedures:

(1) as part of an information security policy for the treatment of personal information; and

(2) that are otherwise consistent with the notification requirements of this chapter;

are considered to be in compliance with this chapter if the agency provides notice required under this chapter in accordance with the agency policy.

SECTION 2. IC 23-15-10 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]:

Chapter 10. Computer System Security Breaches

Sec. 1. (a) As used in this chapter, "breach of the security of the system" means the unauthorized acquisition of computerized data from a computerized data system that compromises the security, confidentiality, or integrity of personal information maintained by a business entity.

(b) The term does not include a good faith acquisition of personal information by an employee or agent of a business entity for business entity purposes if the personal information is not used for or subject to further unauthorized disclosure.

Sec. 2. As used in this chapter, "business entity" means a person that conducts business in Indiana.

Sec. 3. (a) As used in this chapter, "personal information" means:

(1) an individual's unencrypted:

(A) first name or first initial; and

(B) last name; and

(2) at least one (1) of the following:

(A) The individual's unencrypted Social Security number.

(B) The individual's unencrypted driver's license number or identification card number issued under IC 9-24.

(C) The individual's unencrypted:

(i) account number; or

(ii) credit or debit card number;

combined with a required security code, access code, or password that would allow access to the individual's financial account.

(b) The term does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Sec. 4. (a) A business entity that owns or licenses a computerized data system that includes personal information shall disclose any breach of the security of the system after the discovery of the breach to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(b) Subject to section 6 of this chapter, a disclosure made under subsection (a) must be made as soon as possible after the breach is discovered consistent with any measures taken by the business entity that are necessary to:

(1) determine the scope of the breach; and

(2) restore the reasonable integrity of the data system.

Sec. 5. Subject to section 6 of this chapter, a business entity that maintains a computerized data system that includes personal information that the business entity does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following the discovery of the breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Sec. 6. The notification required under sections 4 and 5 of this chapter:

(1) may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; and

(2) shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

Sec. 7. (a) For purposes of sections 4 and 5 of this chapter, notice may be provided by any of the following methods:

(1) Written notice.

(2) Electronic notice if the notice provided is consistent with provisions concerning electronic records and signatures set forth in 15 U.S.C. 7001 et seq.

(3) Another form of notice if the business entity demonstrates that providing notice under subdivisions (1) and (2) would cost more than two hundred fifty thousand dollars ($250,000) or require more than five hundred thousand (500,000) persons to be notified or if the business entity does not have sufficient contact information. Notice provided under this subdivision must include all the following:

(A) Electronic mail notice, if the business entity has an electronic mail address for a person that must be notified.

(B) If the business entity maintains an Internet web site, conspicuous posting of the notice on the business entity's web site.

(C) Notification to major statewide news media.

(b) Notwithstanding subdivision (a), a business entity that maintains its own notification procedures:

(1) as part of an information security policy for the treatment of personal information; and

(2) that are otherwise consistent with the notification requirements of this chapter;

are considered to be in compliance with this chapter if the business entity provides notice required under this chapter in accordance with the business entity policy.

Sec. 8. (a) A person that is injured as the result of a violation of this chapter may bring a civil action:

(1) for injunctive relief against; or

(2) to recover compensatory damages from;

the person that violated this chapter.

(b) An action brought under this section must be commenced not later than two (2) years after the date of the alleged violation.

(c) The remedies provided in this section are not intended to be the exclusive remedies available to a person.

SECTION 3. IC 24-4.8 IS ADDED TO THE INDIANA CODE AS A **NEW** ARTICLE TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]:

ARTICLE 4.8. PROHIBITED SPYWARE

Chapter 1. Definitions

Sec. 1. The definitions in this chapter apply throughout this article.

Sec. 2. "Advertisement" means a communication that has the primary purpose of promoting a commercial product or service.

Sec. 3. (a) "Computer software" means a sequence of instructions written in any programming language that is executed on a computer.

(b) The term does not include computer software that is a web page or a data component of a web page that is not executable independently of the web page.

Sec. 4. "Damage" means a significant impairment to the integrity or availability of data, computer software, a system, or information.

Sec. 5. "Execute" means to perform a function or carry out an instruction of computer software.

Sec. 6. "Intentionally deceptive means" means any of the following:

(1) A materially false statement that a person knows to be false.

(2) A statement or description made by a person who omits or misrepresents material information with the intent to deceive an owner or operator of a computer.

(3) The failure to provide notice to an owner or operator of a computer regarding the installation or execution of computer software with the intent to deceive the owner or operator.

Sec. 7. "Internet" has the meaning set forth in IC 5-22-2-13.5.

Sec. 8. (a) "Owner or operator" means the person who owns or leases a computer, or a person who uses a computer with the authorization of the person who owns or leases the computer.

(b) The term does not include a manufacturer, distributor, wholesaler, retail merchant, or any other person who owns or leases a computer before the first retail sale of the computer.

Sec. 9. "Person" means an individual, a partnership, a corporation, a limited liability company, or another organization.

Sec. 10. "Personally identifying information" means the following information that refers to a person who is an owner or operator of a computer:

(1) Identifying information (as defined in IC 35-43-5-1).

(2) An electronic mail address.

(3) Any of the following information in a form that personally identifies an owner or operator of a computer:

(A) An account balance.

(B) An overdraft history.

(C) A payment history.

Sec. 11. (a) Except as provided in subsection (b), "transmit" means to transfer, send, or otherwise make available computer software or a computer software component through a network, the Internet, a wireless transmission, or any other medium, including a disk or data storage device.

(b) "Transmit" does not include an action by a person who provides:

(1) the Internet connection, telephone connection, or other means of connection for an owner or operator, including a compact disc or DVD on which computer software to establish or maintain a connection is made available;

(2) the storage or hosting of computer software or an Internet web page through which the computer software was made available; or

(3) an information location tool, including a directory, an index, a reference, a pointer, or a hypertext link, through which the owner or operator of the computer located the software;

unless the person receives a direct economic benefit from the execution of the computer software.

Chapter 2. Prohibited Conduct

Sec. 1. This chapter does not apply to a person who monitors or interacts with an owner or operator's Internet connection, Internet service, network connection, or computer if the person is a telecommunications carrier, cable operator, computer hardware or software provider, or other computer service provider who monitors or interacts with an owner or operator's Internet connection, Internet service, network connection, or computer for one (1) or more of the following purposes:

(1) Network security.

(2) Computer security.

(3) Diagnosis.

(4) Technical support.

(5) Maintenance.

(6) Repair.

(7) Authorized updates of software or system firmware.

(8) Authorized remote system management.

(9) Detection or prevention of the unauthorized, illegal, or fraudulent use of a network, service, or computer software, including scanning for and removing computer software that

facilitates a violation of this chapter.

Sec. 2. A person who is not the owner or operator of the computer may not knowingly or intentionally:

(1) transmit computer software to the computer; and

(2) by means of the computer software transmitted under subdivision (1), do any of the following:

(A) Use intentionally deceptive means to modify computer settings that control:

(i) the page that appears when an owner or operator opens an Internet browser or similar computer software used to access and navigate the Internet;

(ii) the Internet service provider, search engine, or web proxy that an owner or operator uses to access or search the Internet; or

(iii) the owner or operator's list of bookmarks used to access web pages.

(B) Use intentionally deceptive means to collect personally identifiable information:

(i) through the use of computer software that records a keystroke made by an owner or operator and transfers that information from the computer to another person; or

(ii) in a manner that correlates the personally identifiable information with data respecting all or substantially all of the web sites visited by the owner or operator of the computer, not including a web site operated by the person collecting the personally identifiable information.

(C) Extract from the hard drive of an owner or operator's computer:

(i) a credit card number, debit card number, bank account number, or any password or access code associated with these numbers;

(ii) a Social Security number, tax identification number, driver's license number, passport number, or any other government issued identification number; or

(iii) the account balance or overdraft history of a person in a form that identifies the person.

(D) Use intentionally deceptive means to prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software.

(E) Knowingly or intentionally misrepresent that computer

software will be uninstalled or disabled by an owner or operator's action.

(F) Use intentionally deceptive means to remove, disable, or otherwise make inoperative security, antispyware, or antivirus computer software installed on the computer.

(G) Take control of another person's computer with the intent to cause damage to the computer or cause the owner or operator to incur a financial charge for a service that the owner or operator has not authorized by:

(i) accessing or using the computer's modem or Internet service; or

(ii) without the authorization of the owner or operator, opening multiple, sequential, standalone advertisements in the owner or operator's Internet browser that a reasonable computer user cannot close without turning off the computer or closing the browser.

(H) Modify:

(i) computer settings that protect information about a person with the intent of obtaining personally identifiable information without the permission of the owner or operator; or

(ii) security settings with the intent to cause damage to a computer.

(I) Prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software by:

(i) presenting an owner or operator with an option to decline installation of computer software knowing that the computer software will be installed even if the owner or operator attempts to decline installation; or

(ii) falsely representing that computer software has been disabled.

Sec. 3. A person who is not the owner or operator may not knowingly or intentionally do any of the following:

(1) Induce the owner or operator to install computer software on the owner or operator's computer by knowingly or intentionally misrepresenting the extent to which installing the computer software is necessary for:

(A) computer security;

(B) computer privacy; or

(C) opening, viewing, or playing a particular type of content.

(2) Use intentionally deceptive means to execute or cause the execution of computer software with the intent to cause the owner or operator to use the computer software in a manner that violates subdivision (1).

Chapter 3. Relief and Damages

Sec. 1. In addition to any other remedy provided by law, a provider of computer software, the owner of a web site, or the owner of a trademark who is adversely affected by reason of the violation may bring a civil action against a person who violates IC 24-4.8-2:

(1) to enjoin further violations of IC 24-4.8-2; and

(2) to recover the greater of:

(A) actual damages; or

(B) one hundred thousand dollars ($100,000);

for each violation of IC 24-4.8-2.

Sec. 2. For purposes of section 1 of this chapter, conduct that violates more than one (1) subdivision, clause, or item of IC 24-4.8-2 constitutes a separate violation for each separate subdivision, clause, or item violated. However, a single action or course of conduct that causes repeated violations of a single subdivision, clause, or item of IC 24-4.8-2 constitutes one (1) violation.

SECTION 4. IC 35-32-2-1 IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]: Sec. 1. (a) Criminal actions shall be tried in the county where the offense was committed, except as otherwise provided by law.

(b) If a person committing an offense upon the person of another is located in one (1) county and ~~his~~ **the person's** victim is located in another county at the time of the commission of the offense, the trial may be in either of the counties.

(c) If the offense involves killing or causing the death of another human being, the trial may be in the county in which the:

(1) cause of death is inflicted;

(2) death occurs; or

(3) victim's body is found.

(d) If an offense is committed in Indiana and it cannot readily be determined in which county the offense was committed, trial may be in any county in which an act was committed in furtherance of the offense.

(e) If an offense is commenced outside Indiana and completed within Indiana, the offender may be tried in any county where any act in furtherance of the offense occurred.

(f) If an offense commenced inside Indiana is completed outside Indiana, the offender shall be tried in any county where an act in furtherance of the offense occurred.

(g) If an offense is committed on the portions of the Ohio or Wabash Rivers where they form a part of the boundaries of this state, trial may be ~~had~~ in the county that is adjacent to the river and whose boundaries, if projected across the river, would include the place where the offense was committed.

(h) If an offense is committed at a place which is on or near a common boundary which is shared by two (2) or more counties and it cannot be readily determined where the offense was committed, then the trial may be ~~had~~ in any county sharing the common boundary.

(i) If an offense is committed on a public highway (as defined in IC 9-25-2-4) that runs on and along a common boundary shared by two (2) or more counties, the trial may be held in any county sharing the common boundary.

(j) If an offense is committed by use of the Internet or another computer network (as defined in IC 35-43-2-3), the trial may be held in any county:

(1) from which or to which access to the Internet or other computer network was made; or

(2) in which any computer, computer data, computer software, or computer network that was used to access the Internet or other computer network is located.

(k) If an offense:

(1) is committed by use of:

(A) the Internet or another computer network (as defined in IC 35-43-2-3); or

(B) another form of electronic communication; and

(2) occurs outside Indiana and the victim of the offense resides in Indiana at the time of the offense;

the trial may be held in the county where the victim resides at the time of the offense.

SECTION 5. IC 35-41-1-1 IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]: Sec. 1. (a) As used in this section, "Indiana" includes:

(1) the area within the boundaries of the state of Indiana, as set forth in Article 14, Section 1 of the Constitution of the State of Indiana;

(2) the portion of the Ohio River on which Indiana possesses concurrent jurisdiction with the state of Kentucky under Article 14, Section 2 of the Constitution of the State of Indiana; and

(3) the portion of the Wabash River on which Indiana possesses concurrent jurisdiction with the state of Illinois under Article 14, Section 2 of the Constitution of the State of Indiana.

(b) A person may be convicted under Indiana law of an offense if:

(1) either the conduct that is an element of the offense, the result that is an element, or both, occur in Indiana;

(2) conduct occurring outside Indiana is sufficient under Indiana law to constitute an attempt to commit an offense in Indiana;

(3) conduct occurring outside Indiana is sufficient under Indiana law to constitute a conspiracy to commit an offense in Indiana, and an overt act in furtherance of the conspiracy occurs in Indiana;

(4) conduct occurring in Indiana establishes complicity in the commission of, or an attempt or conspiracy to commit, an offense in another jurisdiction that also is an offense under Indiana law; ~~or~~

(5) the offense consists of the omission to perform a duty imposed by Indiana law with respect to domicile, residence, or a relationship to a person, thing, or transaction in Indiana;

(6) conduct that is an element of the offense or the result of conduct that is an element of the offense, or both, involve the use of the Internet or another computer network (as defined in IC 35-43-2-3) and access to the Internet or other computer network occurs in Indiana; or

(7) conduct:

(A) involves the use of:

(i) the Internet or another computer network (as defined in IC 35-43-2-3); or

(ii) another form of electronic communication;

(B) occurs outside Indiana and the victim of the offense resides in Indiana at the time of the offense; and

(C) is sufficient under Indiana law to constitute an offense in Indiana.

(c) When the offense is homicide, either the death of the victim or bodily impact causing death constitutes a result under subsection (b)(1). If the body of a homicide victim is found in Indiana, it is presumed that the result occurred in Indiana.

SENATE MOTION

Madam President: I move that Senators Drozda and Broden be added as coauthors of Senate Bill 49.

FORD

COMMITTEE REPORT

Madam President: The Senate Committee on Judiciary, to which was referred Senate Bill No. 49, has had the same under consideration and begs leave to report the same back to the Senate with the recommendation that said bill DO PASS.

(Reference is made to Senate Bill 49 as introduced.)

BRAY, Chairperson

Committee Vote: Yeas 11, Nays 0.

SENATE MOTION

Madam President: I move that Senator Hershman be added as coauthor of Engrossed Senate Bill 49.

FORD

COMMITTEE REPORT

Mr. Speaker: Your Committee on Courts and Criminal Code, to which was referred Senate Bill 49, has had the same under consideration and begs leave to report the same back to the House with the recommendation that said bill be amended as follows:

Delete the title and insert the following:

A BILL FOR AN ACT to amend the Indiana Code concerning computer issues.

Page 1, between the enacting clause and line 1, begin a new paragraph and insert:

"SECTION 1. IC 4-6-6.5 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]:

Chapter 6.5. State Agency Computer System Security Breaches

Sec. 1. (a) As used in this chapter, "breach of the security of the system" means the unauthorized acquisition of computerized data from a computerized data system that compromises the security, confidentiality, or integrity of personal information maintained by a state agency.

(b) The term does not include a good faith acquisition of personal information by an employee or agent of a state agency for agency purposes if the personal information is not used for or subject to further unauthorized disclosure.

Sec. 2. (a) As used in this chapter, "personal information" means:

(1) an individual's unencrypted:

(A) first name or first initial; and

(B) last name; and

(2) at least one (1) of the following:

(A) The individual's unencrypted Social Security number.

(B) The individual's unencrypted driver's license number or identification card number issued under IC 9-24.

(C) The individual's unencrypted:

(i) account number; or

(ii) credit or debit card number;

combined with a required security code, access code, or password that would allow access to the individual's financial account.

(b) The term does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Sec. 3. (a) A state agency that owns or licenses a computerized

data system that includes personal information shall disclose any breach of the security of the system after the discovery of the breach to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(b) Subject to section 5 of this chapter, a disclosure made under subsection (a) must be made as soon as possible after the breach is discovered consistent with any measures taken by the state agency that are necessary to:

(1) determine the scope of the breach; and

(2) restore the reasonable integrity of the data system.

Sec. 4. Subject to section 5 of this chapter, a state agency that maintains a computerized data system that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following the discovery of the breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Sec. 5. The notification required under sections 3 and 4 of this chapter:

(1) may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; and

(2) shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

Sec. 6. (a) For purposes of sections 3 and 4 of this chapter, notice may be provided by any of the following methods:

(1) Written notice.

(2) Electronic notice if the notice provided is consistent with provisions concerning electronic records and signatures set forth in 15 U.S.C. 7001 et seq.

(3) Another form of notice if the state agency demonstrates that providing notice under subdivisions (1) and (2) would cost more than two hundred fifty thousand dollars ($250,000) or require more than five hundred thousand (500,000) persons to be notified or if the agency does not have sufficient contact information. Notice provided under this subdivision must include all the following:

(A) Electronic mail notice, if the agency has an electronic mail address for a person that must be notified.

(B) If the agency maintains an Internet web site, conspicuous posting of the notice on the agency's web site.

(C) Notification to major statewide news media.

(b) Notwithstanding subdivision (a), a state agency that maintains its own notification procedures:

(1) as part of an information security policy for the treatment of personal information; and

(2) that are otherwise consistent with the notification requirements of this chapter;

are considered to be in compliance with this chapter if the agency provides notice required under this chapter in accordance with the agency policy.

SECTION 2. IC 23-15-10 IS ADDED TO THE INDIANA CODE AS A **NEW** CHAPTER TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]:

Chapter 10. Computer System Security Breaches

Sec. 1. (a) As used in this chapter, "breach of the security of the system" means the unauthorized acquisition of computerized data from a computerized data system that compromises the security, confidentiality, or integrity of personal information maintained by a business entity.

(b) The term does not include a good faith acquisition of personal information by an employee or agent of a business entity for business entity purposes if the personal information is not used for or subject to further unauthorized disclosure.

Sec. 2. As used in this chapter, "business entity" means a person that conducts business in Indiana.

Sec. 3. (a) As used in this chapter, "personal information" means:

(1) an individual's unencrypted:

(A) first name or first initial; and

(B) last name; and

(2) at least one (1) of the following:

(A) The individual's unencrypted Social Security number.

(B) The individual's unencrypted driver's license number or identification card number issued under IC 9-24.

(C) The individual's unencrypted:

(i) account number; or

(ii) credit or debit card number;

combined with a required security code, access code, or password that would allow access to the individual's financial account.

(b) The term does not include publicly available information that is lawfully made available to the public from federal, state, or

local government records.

Sec. 4. (a) A business entity that owns or licenses a computerized data system that includes personal information shall disclose any breach of the security of the system after the discovery of the breach to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(b) Subject to section 6 of this chapter, a disclosure made under subsection (a) must be made as soon as possible after the breach is discovered consistent with any measures taken by the business entity that are necessary to:

(1) determine the scope of the breach; and

(2) restore the reasonable integrity of the data system.

Sec. 5. Subject to section 6 of this chapter, a business entity that maintains a computerized data system that includes personal information that the business entity does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following the discovery of the breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Sec. 6. The notification required under sections 4 and 5 of this chapter:

(1) may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; and

(2) shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

Sec. 7. (a) For purposes of sections 4 and 5 of this chapter, notice may be provided by any of the following methods:

(1) Written notice.

(2) Electronic notice if the notice provided is consistent with provisions concerning electronic records and signatures set forth in 15 U.S.C. 7001 et seq.

(3) Another form of notice if the business entity demonstrates that providing notice under subdivisions (1) and (2) would cost more than two hundred fifty thousand dollars ($250,000) or require more than five hundred thousand (500,000) persons to be notified or if the business entity does not have sufficient contact information. Notice provided under this subdivision must include all the following:

(A) Electronic mail notice, if the business entity has an electronic mail address for a person that must be notified.

(B) If the business entity maintains an Internet web site, conspicuous posting of the notice on the business entity's web site.

(C) Notification to major statewide news media.

(b) Notwithstanding subdivision (a), a business entity that maintains its own notification procedures:

(1) as part of an information security policy for the treatment of personal information; and

(2) that are otherwise consistent with the notification requirements of this chapter;

are considered to be in compliance with this chapter if the business entity provides notice required under this chapter in accordance with the business entity policy.

Sec. 8. (a) A person that is injured as the result of a violation of this chapter may bring a civil action:

(1) for injunctive relief against; or

(2) to recover compensatory damages from;

the person that violated this chapter.

(b) An action brought under this section must be commenced not later than two (2) years after the date of the alleged violation.

(c) The remedies provided in this section are not intended to be the exclusive remedies available to a person.

SECTION 3. IC 24-4.8 IS ADDED TO THE INDIANA CODE AS A **NEW** ARTICLE TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2005]:

ARTICLE 4.8. PROHIBITED SPYWARE

Chapter 1. Definitions

Sec. 1. The definitions in this chapter apply throughout this article.

Sec. 2. "Advertisement" means a communication that has the primary purpose of promoting a commercial product or service.

Sec. 3. (a) "Computer software" means a sequence of instructions written in any programming language that is executed on a computer.

(b) The term does not include computer software that is a web page or a data component of a web page that is not executable independently of the web page.

Sec. 4. "Damage" means a significant impairment to the integrity or availability of data, computer software, a system, or information.

Sec. 5. "Execute" means to perform a function or carry out an instruction of computer software.

Sec. 6. "Intentionally deceptive means" means any of the following:

(1) A materially false statement that a person knows to be false.

(2) A statement or description made by a person who omits or misrepresents material information with the intent to deceive an owner or operator of a computer.

(3) The failure to provide notice to an owner or operator of a computer regarding the installation or execution of computer software with the intent to deceive the owner or operator.

Sec. 7. "Internet" has the meaning set forth in IC 5-22-2-13.5.

Sec. 8. (a) "Owner or operator" means the person who owns or leases a computer, or a person who uses a computer with the authorization of the person who owns or leases the computer.

(b) The term does not include a manufacturer, distributor, wholesaler, retail merchant, or any other person who owns or leases a computer before the first retail sale of the computer.

Sec. 9. "Person" means an individual, a partnership, a corporation, a limited liability company, or another organization.

Sec. 10. "Personally identifying information" means the following information that refers to a person who is an owner or operator of a computer:

(1) Identifying information (as defined in IC 35-43-5-1).

(2) An electronic mail address.

(3) Any of the following information in a form that personally identifies an owner or operator of a computer:

(A) An account balance.

(B) An overdraft history.

(C) A payment history.

Sec. 11. (a) Except as provided in subsection (b), "transmit" means to transfer, send, or otherwise make available computer software or a computer software component through a network, the Internet, a wireless transmission, or any other medium, including a disk or data storage device.

(b) "Transmit" does not include an action by a person who provides:

(1) the Internet connection, telephone connection, or other means of connection for an owner or operator, including a compact disc or DVD on which computer software to establish or maintain a connection is made available;

(2) the storage or hosting of computer software or an Internet web page through which the computer software was made

available; or

(3) an information location tool, including a directory, an index, a reference, a pointer, or a hypertext link, through which the owner or operator of the computer located the software;

unless the person receives a direct economic benefit from the execution of the computer software.

Chapter 2. Prohibited Conduct

Sec. 1. This chapter does not apply to a person who monitors or interacts with an owner or operator's Internet connection, Internet service, network connection, or computer if the person is a telecommunications carrier, cable operator, computer hardware or software provider, or other computer service provider who monitors or interacts with an owner or operator's Internet connection, Internet service, network connection, or computer for one (1) or more of the following purposes:

(1) Network security.

(2) Computer security.

(3) Diagnosis.

(4) Technical support.

(5) Maintenance.

(6) Repair.

(7) Authorized updates of software or system firmware.

(8) Authorized remote system management.

(9) Detection or prevention of the unauthorized, illegal, or fraudulent use of a network, service, or computer software, including scanning for and removing computer software that facilitates a violation of this chapter.

Sec. 2. A person who is not the owner or operator of the computer may not knowingly or intentionally:

(1) transmit computer software to the computer; and

(2) by means of the computer software transmitted under subdivision (1), do any of the following:

(A) Use intentionally deceptive means to modify computer settings that control:

(i) the page that appears when an owner or operator opens an Internet browser or similar computer software used to access and navigate the Internet;

(ii) the Internet service provider, search engine, or web proxy that an owner or operator uses to access or search the Internet; or

(iii) the owner or operator's list of bookmarks used to

access web pages.

(B) Use intentionally deceptive means to collect personally identifiable information:

(i) through the use of computer software that records a keystroke made by an owner or operator and transfers that information from the computer to another person; or

(ii) in a manner that correlates the personally identifiable information with data respecting all or substantially all of the web sites visited by the owner or operator of the computer, not including a web site operated by the person collecting the personally identifiable information.

(C) Extract from the hard drive of an owner or operator's computer:

(i) a credit card number, debit card number, bank account number, or any password or access code associated with these numbers;

(ii) a Social Security number, tax identification number, driver's license number, passport number, or any other government issued identification number; or

(iii) the account balance or overdraft history of a person in a form that identifies the person.

(D) Use intentionally deceptive means to prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software.

(E) Knowingly or intentionally misrepresent that computer software will be uninstalled or disabled by an owner or operator's action.

(F) Use intentionally deceptive means to remove, disable, or otherwise make inoperative security, antispyware, or antivirus computer software installed on the computer.

(G) Take control of another person's computer with the intent to cause damage to the computer or cause the owner or operator to incur a financial charge for a service that the owner or operator has not authorized by:

(i) accessing or using the computer's modem or Internet service; or

(ii) without the authorization of the owner or operator, opening multiple, sequential, standalone advertisements in the owner or operator's Internet browser that a reasonable computer user cannot close without turning

off the computer or closing the browser.

(H) Modify:

(i) computer settings that protect information about a person with the intent of obtaining personally identifiable information without the permission of the owner or operator; or

(ii) security settings with the intent to cause damage to a computer.

(I) Prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software by:

(i) presenting an owner or operator with an option to decline installation of computer software knowing that the computer software will be installed even if the owner or operator attempts to decline installation; or

(ii) falsely representing that computer software has been disabled.

Sec. 3. A person who is not the owner or operator may not knowingly or intentionally do any of the following:

(1) Induce the owner or operator to install computer software on the owner or operator's computer by knowingly or intentionally misrepresenting the extent to which installing the computer software is necessary for:

(A) computer security;

(B) computer privacy; or

(C) opening, viewing, or playing a particular type of content.

(2) Use intentionally deceptive means to execute or cause the execution of computer software with the intent to cause the owner or operator to use the computer software in a manner that violates subdivision (1).

Chapter 3. Relief and Damages

Sec. 1. In addition to any other remedy provided by law, a provider of computer software, the owner of a web site, or the owner of a trademark who is adversely affected by reason of the violation may bring a civil action against a person who violates IC 24-4.8-2:

(1) to enjoin further violations of IC 24-4.8-2; and

(2) to recover the greater of:

(A) actual damages; or

(B) one hundred thousand dollars ($100,000);

for each violation of IC 24-4.8-2.

Sec. 2. For purposes of section 1 of this chapter, conduct that violates more than one (1) subdivision, clause, or item of IC 24-4.8-2 constitutes a separate violation for each separate subdivision, clause, or item violated. However, a single action or course of conduct that causes repeated violations of a single subdivision, clause, or item of IC 24-4.8-2 constitutes one (1) violation.".

Renumber all SECTIONS consecutively.

and when so amended that said bill do pass.

(Reference is to SB 49 as printed January 14, 2005.)

ULMER, Chair

Committee Vote: yeas 11, nays 0.